UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/754,402	01/09/2004	Dennis Michael Volpano	324413.06/MFCP.141333	7973

45809 7590 09/01/2009

SHOOK, HARDY & BACON L.L.P.
(c/o MICROSOFT CORPORATION)
INTELLECTUAL PROPERTY DEPARTMENT
2555 GRAND BOULEVARD
KANSAS CITY, MO 64108-2613

EXAMINER	
BROOKS, SHANNON	

ART UNIT	PAPER NUMBER
2617	

MAIL DATE	DELIVERY MODE
09/01/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/754,402	VOLPANO, DENNIS MICHAEL	
	Examiner	Art Unit	
	SHANNON R. BROOKS	2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 July 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,7,53 and 56-70* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,7,53 and 56-70* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 January 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *6/26/09*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114 was filed in this application after appeal to the Board of Patent Appeals and Interferences, but prior to a decision on the appeal. Since this application is eligible for continued examination under 37 CFR 1.114 and the fee set forth in 37 CFR 1.17(e) has been timely paid, the appeal has been withdrawn pursuant to 37 CFR 1.114 and prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on 7/20/09 has been entered.

Claim Rejections - 35 USC § 102

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. **Claims 56-65** are rejected under 35 U.S.C. 102(e) as being anticipated by Kitchin (US 7130904 B2).

Consider **Claim 56**, Kitchin teaches A secure wireless network, comprising:

a virtual 802.11 Basic Service Set (BSS) (appears as multiple logical sets (Col. 6, lines 1-47);

a plurality of stations in the virtual BSS, each of said stations having a hardware media access control (MAC) address (Col. 6, lines 16-23);

all said stations in said virtual BSS sharing a group security association wherein said group

security association is an implementation of a MAC security (a logical access point for a class of subscribers (Col. 6, lines 16-47); and one of said stations in said virtual BSS comprising an access point (Col. 6, lines 1-47).

Consider **Claim 57**, Kitchin teaches the network of claim 56, wherein said implementation of said MAC security comprises said implementation of a secure MAC service (Col. 6, lines 16-47).

Consider **Claim 58**, Kitchin teaches the network of claim 57, wherein said implementation of said secure MAC service comprises a MAC Security Key Agreement and a MAC Security Entity (Col. 6, lines 1-67) .

Consider **Claim 59**, Kitchin teaches the network of claim 57, wherein said group security association (a logical access point for a group of subscribers) comprises using one or more cryptographic methods (encryption key, Col. 6, line 16-47).

Consider **Claim 60**, Kitchin teaches the network of claim 59, further comprising the one or more cryptographic methods implemented in a security relationship maintained by a MAC Security Key Agreement (Col. 6, lines 1-47).

Consider **Claim 61**, Kitchin teaches a method in an access point device for a secure wireless network to support segregation of network traffic among a plurality of stations, each of said stations having a hardware media access control (MAC) address (Col. 6, lines 16-47), comprising:

receiving an association request or a probe request from a first station (access point is associated with one or more BSS, Col. 6, lines 1-7 or set of beacons containing BSSID or ESSID, Col. 6, lines 47-67); determining for said request a basic service set (BSS) that is unknown to said

access point device at a time said request was received by said access point device (defining a security policy that ensures that unauthorized clients and subscibers do not have access, Col. 6, lines 16-27);

receiving at least one parameter which defines said BSS (BSS associated with a distinct MAC address or group, Col. 6, lines 16-24);

establishing said BSS based at least on said at least one parameter, thereby creating said BSS for a subset of said stations (BSS associated with a distinct MAC address or group, Col. 6, lines 16-24); and sending a response to said end station that includes a BSSID of said established BSS (Col. 6, lines 47-63);

wherein stations in said subset belong to said established BSS and share a group security association wherein said group security association is an implementation of a MAC security (BSS belong to a particular class of subscriber or client, Col. 6, lines 1-15).

Consider **Claim 62**, Kitchin teaches the method of claim 61, wherein said implementation of said MAC security comprises said implementation of a secure MAC service (Col. 6, lines 16-47).

Consider **Claim 63**, Kitchin teaches the method of claim 62, wherein said implementation of said secure MAC service comprises a MAC Security Key Agreement and a MAC Security Entity (Col. 6, lines 1-67).

Consider **Claim 64**, Kitchin teaches the method of claim 62, wherein said group security association (each BSS defines a logical access point for a class of clients or subscribers, Col. 6,

lines 16-47) comprises using one or more cryptographic methods (encryption key, Col. 6, lines 16-47).

Consider **Claim 65**, Kitchin teaches the method of claim 64, further comprising the one or more cryptographic methods implemented in a security relationship maintained by a MAC Security Key Agreement (Col. 6, lines 1-47).

3. **Claims 66-70** are rejected under 35 U.S.C. 102(e) as being anticipated by Halasz (US 7194622 B1).

Consider **Claim 66**, Halasz teaches an access point for segregating traffic among a plurality of end

stations (col. 6, lines 48-67), comprising:

one or more storage units configurable to store:

a frame having a cryptographic authentication code (authentication server can be co-located at AP, Col. 5, lines 26-55);
the frame having a source media access control (MAC) address (Col. 5, lines 64-67) to determine a preliminary VLAN classification (Col. 5, line 56-Col. 7, line 16) when the frame carries a null virtual LAN ID (not valid, Col. 6, lines 45-52) ; the frame having a virtual LAN ID (VID) as the preliminary VLAN classification when the frame carries the VID (Col. 5, line 56-Col. 7, line 16); a table of security associations providing a cryptographic authentication code key based on the preliminary VLAN classification wherein the cryptographic authentication code key is used to recompute a new cryptographic authentication code over a payload of the frame

(Col. 5, line 56-Col. 7, line 31); the new cryptographic authentication code compared with the cryptographic authentication code (determining based on credentials, Col. 5, lines 33-Col. 7, line 31);

the preliminary VLAN classification implemented as a final VLAN classification when the new cryptographic authentication code and the cryptographic authentication code match, wherein the frame is decrypted (determining based on credentials, Col. 5, lines 33-Col. 7, line 31); and the preliminary VLAN classification not implemented as the final VLAN classification when the new cryptographic authentication code and the cryptographic authentication code do not match, wherein the frame is discarded (determining based on credentials or VLAN ID invalid due to roaming or nonauthentications are blocked, Col. 5, lines 33-Col. 7, line 31).

Consider **Claim 67**, Halasz teaches the access point of claim 66, wherein the access point is configurable to perform an authentication operation (authentication server can be co-located at AP, Col. 5, lines 26-55) that generates the authentication code key (Col. 5, lines 1-55).

Consider **Claim 68**, Halasz teaches the access point of claim 66, wherein the new cryptographic authentication code is recomputed over the payload using a cryptographic message digest algorithm determined during an initial authentication operation (when credentials are presented by supplicant and must be authorized within a time period, Col. 5, lines 1-55).

Consider **Claim 69**, Halasz teaches the access point of claim 66, wherein the final VLAN classification is used as a value of a VLAN classification parameter of any corresponding data request primitives (Col. 5, line 56-Col. 7, line 24).

Consider **Claim 70**, Halasz teaches the access point of claim 66, wherein the cryptographic authentication code or the new cryptographic authentication code uniquely identifies the VLAN (Col. 5, line 56-Col. 7, line 24).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 1, 2, and 7** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kitchin (US 7130904) in view of Meier (US 6847620 B1) and further in view of Halasz (US 7194622 B1).

Consider **Claim 1**, Kitchin teaches an access point device for a wireless LAN for isolating an end station from a plurality of end stations to support segregation of network traffic between the end station and the plurality of end stations, the access point device serving as a common access point for communication in the wireless LAN (Col. 3, line 51-Col. 4, line 52), the access point configured to: receive a request from said end station that is an association request or a probe request (Col. 6, lines 16-26); and process said request by:

receiving at least one parameter defining said BSS (read as associating a BSS with a class of subscribers or clients, Pg. 6, lines 1-15 or BSSID or ESSID, Col. 6, lines 47-67);

establishing said BSS based at least on said at least one parameter (read as established based on class of client or subscriber, Pg. 6, lines 1-15 or BSSID or ESSID, Col. 6, lines 47-67); and sending a response to said end station that includes a BSSID of said established BSS (Pg. 6, lines 47-67);

except that Kitchin does not specifically teach determining for said request a basic service set (BSS) that is unknown to said access point device at the time of receipt of said request by said access point device; nor does it specifically teach establishing a security association with said end station within said BSS wherein the security association includes at least two keys, one key for encryption and another key for computing an authentication code;

.

However, Meier teaches determining for said request a basic service set (BSS) that is unknown (read as roaming and not known when received and possibly belonging to a remote subnet, Col. 17, lines 1-49) to said access point device at the time of receipt of said request by said access point device (read as, at time of receipt, a frame does not contain a VLAN-ID for a recognizable VLAN subnet and therefore must undergo a matching process, Col. 17, lines 1-49).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to incorporate the teachings of Meier with Kitchin in order to aid in identifying the correct subnet-ID/VLAN binding (Col. 17, lines 2-15).

Kitchin and Meier do not specifically teach establishing a security association with said end station within said BSS wherein the security association includes at least two keys, one key for encryption and another key for computing an authentication code.

However, Halasz teaches establishing a security association with said end station within said BSS wherein the security association includes at least two keys, one key for encryption and another key for computing an authentication code (Col. 5, line 1-Col. 6, line 2).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to incorporate the teaching of Halasz into Kitchin and Meier to aid in establishing security (Col. 5, line 1-Col. 6, line 2).

Consider **Claim 7**, Kitchin teaches a method in an access point device for a secure wireless network to support segregation of network traffic among a plurality of stations, each of said stations having a hardware (MAC) address (Col. 6, lines 16-26), comprising:

receiving an association request or a probe request from a first station (read as accessibility via access point from beacon, Col. 6, lines 47-67);

receiving at least one parameter defining said BSS (read as BSSID or ESSID,. Col. 6, lines 47-67);

establishing said BSS based at least on said at least one parameter, thereby creating a Basic Service Set (BSS) for a subset of said stations, and sending a response to said end station

that includes a BSSID of said established BSS (read as BSS established based on class of client or subscriber, Pg. 6, lines 1-15 or BSSID or ESSID, Col. 6, lines 47-67), wherein stations in said subset belong to said established BSS and share a group security association (Col. 6, lines 16-47);

except that Kitchin does not specifically teach determining for said request a basic service set (BSS) that is unknown to said access point device at the time said request was received by said access point device ; nor does it specifically teach establishing a security association with said end station within said BSS wherein the security association includes at least two keys, one key for encryption and another key for computing an authentication code;

However, Meier teaches determining for said request a basic service set (BSS) that is unknown (read as roaming and not known when received and possibly belonging to a remote subnet, Col. 17, lines 1-49) to said access point device at the time of receipt of said request by said access point device (read as, at time of receipt, a frame does not contain a VLAN-ID for a recognizable VLAN subnet and therefore must undergo a matching process, Col. 17, lines 1-49).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to incorporate the teachings of Meier with Kitchin in order to aid in identifying the correct subnet-ID/VLAN binding (Col. 17, lines 2-15)

Kitchin and Meier do not specifically teach establishing a security association with said end station within said BSS wherein the security association includes at least two keys, one key for encryption and another key for computing an authentication code.

However, Halasz teaches establishing a security association with said end station within said BSS wherein the security association includes at least two keys, one key for encryption and another key for computing an authentication code (Col. 5, line 1-Col. 6, line 2).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to incorporate the teaching of Halasz into Kitchin and Meier to aid in establishing security (Col. 5, line 1-Col. 6, line 2).

Consider **Claim 2**, Kitchin teaches the access point device , further configured to provision a plurality of separate LAN segments **(read as distinct physical media, Col. 4, lines 4-6)** while providing separate link privacy and integrity for each of said LAN segments **(Col. 6, lines 16-26).**

6. **Claim 53 is** rejected under 35 U.S.C. 103(a) as being unpatentable over Kitchin (US 7130904) in view of Meier (US 6847620 B1) and further in view Halasz (US 7194622 B1) and still further in view of of Kimura (US 2001/0048744 A1).

Consider **Claim 53**, Kitchin and Meier and Halasz teach the access point device of Claim 1 except that the combination does not specifically teach wherein said request includes an SSID (service set identifier), wherein said at least one parameter is based on said SSID (Col. 6, lines 47-67).

However, Kimura teaches wherein said request includes an SSID (service set identifier) (Pg. 1, [0006], Pg. 2, [0014], and Pg. 4, [0045], wherein said at least one parameter is based on said SSID (Fig. 2, item 21] and Pg. 1, [0012])).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to incorporate the teachings of Kitchin, Meier, and Halasz into Kimura in order to aid in the association process (Pg. 2, [0014]).

Conclusion

Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to:**

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window

Randolph Building

401 Dulany Street

Alexandria, VA 22314

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shannon Brooks whose telephone number is (571) 270-1115. The examiner can normally be reached on 7:30a.m. to 5p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nick Corsaro can be reached on (571) 272-7876. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist/customer service whose telephone number is (571) 272-2600.

/Shannon R. Brooks/

Examiner, Art Unit 2617

Shannon Brooks

August 29, 2009

/NICK CORSARO/

Supervisory Patent Examiner, Art Unit 2617